significantly in recent years, including for debit cards used in ewallets such as Apple Pay, Google Pay, and Samsung Wallet.

When a cardholder loads a debit card into an ewallet, the debit card is "tokenized," meaning the primary account number ("PAN") printed on the card is replaced with a different number—the "token"—to protect the PAN during certain stages of a debit transaction. The token service provider ("TSP") that generates the token also maintains a "token vault" that stores the PAN corresponding to each token. When a cardholder initiates a debit transaction using an ewallet, the merchant receives only the token, and not the PAN. The merchant sends this token to its acquirer, which sends the token to a network for processing. For the transaction to proceed, the TSP must "detokenize" the token for the network, which includes converting the token to its associated PAN stored in the token vault.

Mastercard's rules require that a Mastercard-branded debit card that is loaded into an ewallet be tokenized. Mastercard is also the TSP for nearly all Mastercard-branded debit cards used in ewallets. When an ewallet transaction using a Mastercard-branded debit card is routed to Mastercard, Mastercard thus can perform the detokenization and process the transaction. Competing payment card networks, however, do not have access to Mastercard's token vault. To route a Mastercard-branded tokenized transaction to a competing network, a merchant's acquirer or the competing network therefore must ask Mastercard to detokenize the token. Merchants are thus dependent on Mastercard's detokenization to route ewallet transactions using Mastercard-branded debit cards to competing networks.

Mastercard's ewallet token policy leverages tokens to protect its card-not-present ecommerce revenue by inhibiting merchants' ability to route such transactions to competing networks. For card-present debit transactions using an ewallet—which occur when a cardholder makes a purchase in-store by holding their mobile phone with an ewallet application to a merchant's terminal—Mastercard will detokenize so that merchants may route the transactions to competing networks. In this scenario, the merchant's acquirer or competing network will "call out" to Mastercard's token vault, which will provide the PAN associated with the token.

In contrast, Mastercard will not detokenize for card-not-present (ecommerce) debit transactions, including those using an ewallet. Under Mastercard's policy, there is no process by which a merchant's acquirer or a competing network can call out to Mastercard's token vault and obtain the PAN associated with an ewallet token used in a card-not-present debit transaction, as it can in a card-present transaction. Thus, when a Mastercard-branded card is used in an ewallet for a card-not-present debit transaction, that transaction must be routed over the Mastercard network, and merchants are unable to route transactions to competing networks. Indeed, Mastercard requires, and affirmatively tells merchants that it requires, that merchants route card-not-present ewallet transactions using Mastercard-branded debit cards to the Mastercard network.

For purposes of the Durbin Amendment and Regulation II, a "debit card" includes more than the physical piece of plastic found in a cardholder's wallet. Under both, a debit card is "any card, or device, issued or approved for use through a payment card network to debit an account, regardless of whether authorization is based on signature, personal identification number (PIN), or other means, and regardless of whether the issuer holds the account."[7] Ewallet tokens are payment codes stored inside an ewallet and used through a payment card network to debit a cardholder's account; they are thus debit cards governed by the Durbin Amendment and Regulation II.

Mastercard's ewallet token policy does not allow card-not-present debit transactions using ewallet tokens (, debit cards) to be routed to competing debit networks. A merchant thus has only one option: Mastercard's network. Mastercard's policy thereby inhibits the merchant's ability to direct the routing of card-not-present transactions using ewallet tokens over the available network of its choosing, in violation of the Durbin Amendment and Regulation II.

Even if, for the sake of argument, an ewallet token is characterized not as a debit card but as a means of access to the underlying PAN, Mastercard still unlawfully inhibits merchant routing choice with respect to card-not-present ewallet transactions. Mastercard requires that all Mastercard-branded debit cards loaded into ewallets be tokenized. And, in fact, nearly all such cards are tokenized by Mastercard—via decisions in which merchants have no say. Because Mastercard tokenizes these cards and then withholds detokenization, card-not-present ewallet transactions are not routable to competing networks—these networks are unable to process the transactions without the corresponding PANs. Mastercard thereby inhibits merchant routing choice by employing a technology that compels merchants to route transactions over Mastercard's network.

Additionally, Mastercard's agreements with ewallet providers require those providers to inform merchants that, by accepting card-not-present transactions through ewallets, merchants agree that transactions made with Mastercard-branded debit cards will be routed to Mastercard. Mastercard thereby inhibits merchant routing choice by contract.

The proposed order seeks to remedy Mastercard's illegal conduct by requiring Mastercard to provide PANs so that merchants may route tokenized transactions using Mastercard-branded debit cards to the available network of their choosing. Under the proposed order, Mastercard must also refrain from interfering with the ability of other persons to serve as TSPs, and it must not take other actions to inhibit merchant routing choice in violation of Regulation II, 12 C.F.R. § 235.7(b).

Section I of the proposed order defines the key terms used in the order.

Section II of the proposed order addresses the core of Mastercard's conduct. Paragraph II.A. requires Mastercard, upon request by an authorized acquirer, authorized network, or other authorized person in receipt of a Mastercard token, to provide the PAN

associated with the token for purposes of routing the transaction to any competing network enabled by the issuer